

118TH CONGRESS
2D SESSION

S. _____

To require Federal contractors to implement a vulnerability disclosure policy consistent with NIST guidelines, and for other purposes.

IN THE SENATE OF THE UNITED STATES

Mr. WARNER introduced the following bill; which was read twice and referred to the Committee on _____

A BILL

To require Federal contractors to implement a vulnerability disclosure policy consistent with NIST guidelines, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Federal Contractor
5 Cybersecurity Vulnerability Reduction Act of 2024”.

6 **SEC. 2. FEDERAL CONTRACTOR VULNERABILITY DISCLO-**
7 **SURE POLICY.**

8 (a) RECOMMENDATIONS.—

9 (1) IN GENERAL.—Not later than 180 days
10 after the date of the enactment of this Act, the Di-

1 rector of the Office of Management and Budget, in
2 consultation with the Director of the Cybersecurity
3 and Infrastructure Security Agency, the National
4 Cyber Director, the Director of the National Insti-
5 tute of Standards and Technology, and any other
6 appropriate head of an Executive department,
7 shall—

8 (A) review the Federal Acquisition Regula-
9 tion (FAR) contract requirements and language
10 for contractor vulnerability disclosure programs;
11 and

12 (B) recommend updates to such require-
13 ments and language to the Federal Acquisition
14 Regulation Council.

15 (2) CONTENTS.—The recommendations re-
16 quired by paragraph (1) shall include updates to
17 such requirements designed to ensure that covered
18 contractors implement a vulnerability disclosure pol-
19 icy consistent with National Institute of Standards
20 and Technology (NIST) guidelines for contractors as
21 required under section 5 of the IoT Cybersecurity
22 Improvement Act of 2020 (15 U.S.C. 278g–3c).

23 (b) PROCUREMENT REQUIREMENTS.—Not later than
24 180 days after the date on which the recommended con-
25 tract language developed pursuant to subsection (a) is re-

1 ceived, the Federal Acquisition Regulation Council shall
2 review the recommended contract language and amend the
3 FAR as necessary to incorporate requirements for covered
4 contractors to solicit and address information about poten-
5 tial security vulnerabilities relating to an information sys-
6 tem owned or controlled by the contractor that is used
7 in performance of a Federal contract.

8 (c) ELEMENTS.—The update to the FAR pursuant
9 to subsection (b) shall—

10 (1) to the maximum extent practicable, align
11 with the security vulnerability disclosure process and
12 coordinated disclosure requirements relating to Fed-
13 eral information systems under sections 5 and 6 of
14 the IoT Cybersecurity Improvement Act of 2020 (15
15 U.S.C. 278g–3c, 278g–3d); and

16 (2) to the maximum extent practicable, be
17 aligned with industry best practices and Standards
18 29147 and 30111 of the International Standards
19 Organization (or any successor standard) or any
20 other appropriate, relevant, and widely used stand-
21 ard.

22 (d) WAIVER.—The head of an agency may waive the
23 security vulnerability disclosure policy requirement under
24 subsection (b) if the agency Chief Information Officer—

1 (1) determines that the waiver is necessary in
2 the interest of national security or research pur-
3 poses; and

4 (2) not later than 30 days after granting the
5 waiver, submits a notification and justification, in-
6 cluding information about the duration of the waiv-
7 er, to the Committee on Homeland Security and
8 Governmental Affairs of the Senate and the Com-
9 mittee on Oversight and Accountability of the House
10 of Representatives.

11 (e) DEPARTMENT OF DEFENSE SUPPLEMENT TO
12 THE FEDERAL ACQUISITION REGULATION.—

13 (1) REVIEW.—Not later than 180 days after
14 the date of the enactment of this Act, the Secretary
15 of Defense shall review the Department of Defense
16 Supplement to the Federal Acquisition Regulation
17 (DFARS) contract requirements and language for
18 contractor vulnerability disclosure programs and de-
19 velop updates to such requirements designed to en-
20 sure that covered contractors, to the maximum ex-
21 tent practicable, align with the security vulnerability
22 disclosure process and coordinated disclosure re-
23 quirements relating to Federal information systems
24 under sections 5 and 6 of the IoT Cybersecurity Im-

1 provement Act of 2020 (15 U.S.C. 278g–3c, 278g–
2 3d).

3 (2) REVISIONS.—Not later than 180 days after
4 the date on which the review required under sub-
5 section (a) is completed, the Secretary shall revise
6 the DFARS as necessary to incorporate require-
7 ments for covered contractors to receive information
8 about a potential security vulnerability relating to an
9 information system owned or controlled by a con-
10 tractor, in performance of the contract.

11 (3) ELEMENTS.—The Secretary shall ensure
12 that the revision to the DFARS described in this
13 subsection is carried out in accordance with the re-
14 quirements of paragraphs (1) and (2) of subsection
15 (c).

16 (4) WAIVER.—The Chief Information Officer of
17 the Department of Defense may waive the security
18 vulnerability disclosure policy requirements under
19 paragraph (2) if the Chief Information Officer—

20 (A) determines that the waiver is necessary
21 in the interest of national security or research
22 purposes; and

23 (B) not later than 30 days after granting
24 the waiver, submits a notification and justifica-
25 tion, including information about the duration

1 of the waiver, to the Committee on Armed Serv-
2 ices of the Senate and the Committee on Armed
3 Services of the House of Representatives.

4 (f) DEFINITIONS.—In this section:

5 (1) AGENCY.—The term “agency” has the
6 meaning given the term in section 3502 of title 44,
7 United States Code.

8 (2) COVERED CONTRACTOR.—The term “cov-
9 ered contractor” means a contractor (as defined in
10 section 7101 of title 41, United States Code)—

11 (A) whose contract is in an amount the
12 same as or greater than the simplified acquisi-
13 tion threshold; or

14 (B) that uses, operates, manages, or main-
15 tains a Federal information system (as defined
16 by section 11331 of title 40, United States
17 Code) on behalf of an agency.

18 (3) EXECUTIVE DEPARTMENT.—The term “Ex-
19 ecutive department” has the meaning given that
20 term in section 101 of title 5, United States Code.

21 (4) SECURITY VULNERABILITY.—The term “se-
22 curity vulnerability” has the meaning given that
23 term in section 2200 of the Homeland Security Act
24 of 2002 (6 U.S.C. 650).

1 (5) SIMPLIFIED ACQUISITION THRESHOLD.—
2 The term “simplified acquisition threshold” has the
3 meaning given that term in section 134 of title 41,
4 United States Code.